~~TOP SECRET~~ TICOM/D-41

TRANSLATION OF CRYPTANALYTIC REPORTS BY OKM 4/SKL III ON BRITISH NAVAL SYSTEMS, FROM FOLDER ENTITLED "RESEARCH PROGRESS 1/12/43 - 1/11/44", TICOM DOCUMENT, NO T 519

I. Progress Report by the "5-figure Party", 2/11/44.

II. General Survey of Research by section III F in 1943, 5/1/44.

III. Routine Report on C.C.M., 7/11/44.

IV. Progress Report on Naval Shore Code and Naval Code, 1/11/44.

V. Progress Report for Delivery Groups and "Turkey", 2/11/44.

TICOM
August, 1945

No. of pages: 6

DISTRIBUTION:

British

D.D.3
D.D.4
D.D.(N.S.)
D.D.(M.W.)
D.D.(A.S.)
Cdr. Tandy
Major Morgan
Miss Mortimer (2)

U.S.

Op-20-G (2) (via Lt.Cdr.Manson)
G-2 (via Lt.Col.Hilles)
A.S.A. (3) (via Major Seaman)
Director, S.I.D. USFET (via Lt.Col.Johnson)
Col. Lewis Powell, USSTAF.

TICOM

Chairman
S.A.C.
Cdr. Bacon
Lt. Col. Johnson
Major Seaman
Lt. Cdr. Manson
Capt. King
Ticom Files (2)

ADDITIONAL

S.A.C. for D.S.D.10 Admiralty
S.A.C. for D.D.(C.S.A.)
S.A.C. for D.S.D.4X

I

~~TOP SECRET~~

OKM 2/11/44

4/SKL III Fm

To: 4/SKL III

4589

PROGRESS REPORT ON THE "5 - FIGURE PARTY" FOR 1/11/44

A decoded LC..O message of 23/10/44 confirms the discovery, mentioned in the last report, that the "future arrangements" for Naval Code (with auxiliary tables) proposed in the S.F.O. have come into force.

The examination of the September and October material of Naval Code (with general tables) has shown that the old allocation of areas has been discontinued for this system too. Very many 5-figure families, each of a large size, and which do not fit into the previously known arrangement can be distinguished. It cannot yet be stated with certainty whether this indicates the introduction of the "future arrangements" for this system too, for, there are no signs yet of a "world-wide" use of recypher tables B, K, X and Y, which was to take place upon the introduction of the "future arrangements".

No new data for Naval Cypher. A new task is the attempt to separate the 5-figure groups belonging to recypher table "S" (Area 1) from the rest of the material.

An examination of the "One-time Pads" (wireless messages with 6, 7 and 8-symbol indicators) has revealed the following:

One-time Pad "Navy Six" (S.P. 02392) is the one most frequently used. There are at least 32 tables in use at the same time, some of them in the MEDITERRANEAN and some on the Invasion Coast. Naval Shore Code (system "STETTIN") is used for cable messages recyphered by tables 448, 451 and 678.

One-time Pads "Navy Three" (S.P. 02389) and "Navy Twenty" (S.P. 02457) were intercepted less frequently. The former appears in traffic between U.K. and ALEXANDRIA and MURMANSK, the latter in RINELLA-ALEXANDRIA and WHITEHALL-POLYARNCE traffic. (Distribution: S.B.N.O. MURMANSK).

One Time Pad "Navy Two" (S.P. 02341) is mostly transmitted with a 5-figure indicator. All attempts to identify it among the 5-figure material received were in vain.

It appeared in moderate numbers with a 6-figure indicator.

In addition it was established that the 4-figure groups transmitted with the indicator "morse" are One Time Pads.

/TYPE X

TYPE X

Of the messages encoded with the English "Type X" machine, 24,303 were received in September. Principal area of incidence: MEDITERRANEAN (8,253 wireless messages) and East INDIA (7,317 wireless messages). A comparison with the main British systems Naval Cypher and Naval Code of which 40,500 wireless messages were intercepted, shows that Type X is much less frequently used than these.

II

In the field, 5th January, 1944

SKL/Chef MND III F

~~TOP SECRET~~

RESEARCH (SECTION III F) IN 1943

1) The recyphering of the starting point indicator groups introduced into the main British systems on 15th December, 1942 dominated research work during the whole of 1943. The outcome of our 1941 experiences, which had shown that when the indicator groups are recyphered, only relatively large employment of personnel can produce results of any operational importance at all, was repeated in the later period.

2) The main problem was to increase personnel working on Naval Cypher No. 3 system, in order to achieve cryptanalytic results in good time, since this was the most important system for the conduct of the U-Boat war. This increase of personnel could only be obtained by taking everyone working on the other Naval Cypher, since there were no reserves available. The staff thus doubled in size was nevertheless still quite inadequate; operationally useful results were only obtained by trebling the staff and getting the utmost work out of the punched card party.

The Naval Cypher No. 3 basic code book changed on 10th June. In spite of great efforts being made, it was impossible to break into the system during 1943.

3) Owing to the staff shortage, and to the already familiar difficulties ensuing from the recypherment of the indicator groups, work on the other Naval Cypher was suspended at the beginning of the year, and was not resumed in 1943.

The basic code book changed on 10th June, at the same time as Naval Cypher No. 3. At this point, in the place of the two Naval Cyphers one common basic book was introduced, henceforth known to us as FRANKFURT.

4) The Naval Code basic book captured towards the end of 1942 remained in force until 28/2. In the FREETOWN area only it remained in use until 19/4, with the old keys (Schlüsselmittel) of the second half of February.

Up till the change, Naval Code (with Gen. Tables) by the decypherment of addresses, was used almost exclusively to establish the dispositions of the British main units. After the change, 7 months were necessary, using as much personnel as possible, before we could read the new basic code book.

Whereas Naval Code (with Aux. Tables) could be read relatively quickly and extensively after the break, unforeseen

/difficulties

difficulties arose with Naval Code (with Gen. Tables) presumably ascribable to certain complications in the recypher system.

On 1/12 an alteration of the recypher system was introduced, whereby Naval Code (with Aux. Tables) daily key used one subtractor for both address and text.

5) The British machine cypher (Type X) was increasingly used for traffic between shore stations.

6) The Fleet Code continued to be used unrecyphered. Cypher security, insofar as this is of operational necessity, is guaranteed by the fact that the system is little used, and is changed at short intervals.

7) The D/F system continued to be used for the transmission of single D/F reports. One time pads are also being extensively used with this system.

8) During the spring, the Inter-Departmental Cypher was replaced by the Inter Service Cypher. This system is used for traffic between the different branches of the armed forces. We could do nothing with it, as the volume of traffic was too slight.

9) Naval Shore Code, used by shore stations and by Reporting Officers at Consulates, was worked on for a time, as far as the Reporting Officers' traffic was concerned, but without visible success, as the material received from this sphere is too slight. The traffic from the actual Naval stations is outwardly indistinguishable from the main systems, and is thus hard to recognise. One time pads are extensively used.

10) In the middle of the Summer, a copy of the special code used for traffic between SCAPA FLOW and units of 30th M.T.B. flotilla was captured from a M.T.B. in the Norwegian area. The system is recyphered exclusively on a one time pad. Important findings were nevertheless collected from the captured material, so that later it was possible to establish the presence at sea of boats of this flotilla by the external characteristics of the W/T messages.

11) At the beginning of November we captured from the fast blockade runner MASTER STANDFAST a special code used for the traffic between the Admiralty and the blockade runner flotilla and the steamers DICTO and LIONEL lying in Swedish ports. The system is outwardly identical with MERSIGS, but is used unrecyphered.

12) In the middle of the Summer, in response to a demand from the U-Boat operational command, an examination of British weather systems was undertaken. From this it emerged that most weather reports are recyphered on one time pads. The remaining material hardly suffices for working on.

13) In February, a "one time" table 150 groups long was introduced into the MERSIGS system for shore stations controlling convoys. As more than 150 groups are sent for most convoys, current and rapid breaking was possible.

Positions given at the beginning of messages according to latitude and longitude were given in relation to fixed points after 1/12.

In the general MERSIGS system, a slow change-over from letters to figures took place during the course of the year, and was completed by the end of September. The indicator group system remained independent of this change-over, and did not alter.

14) The two-letter LOXO system changed its basic code book (to 3-letter LOXO-FOXO) and for operational W/T traffic even the system was changed (to COFOX - MEDOX). Knowledge of the routines prevented any cryptanalytic break down.

15) The Examination and Naval Control Service Code ((ECCO)) went out of use in September. The traffic went over to LOXO.

16) NYKO and CYKO systems were still only used separately. In the middle of the year, a new 3-letter system appeared for these, based on a daily changing basic code book and a recypherment of the Air Force Code.

17) The system used for torpedo carrying a/c practice in the NORTH CHANNEL, was read currently.

18) The key-periods for the International BENTLY Code were reduced from the initial six weeks to three and later even to two weeks. This system gave valuable insight into the shipping situation in the Near and Middle East.

19) Government Telegraph Code continued to be used only for sending Navicerts and reports on shipping questions.

III

~~TOP SECRET~~

4/SKL III Fl. 7/11/44

STATE OF CRYPTANALYSIS ON THE COMBINED

CYPHER MACHINE

Investigations have so far produced no fresh results. Traffic at present is heavy (up to 200 messages daily).

IV TOP SECRET

4/SKL III Fn In the Field, 2/11/44

To: 4/SKL III

((1)) PROGRESS REPORT ON Naval Shore Code FOR 1/11/44

About 100 relative book groups were recovered. A start was made on the interpretation of these groups. Complete results, of use for operational evaluation, cannot be expected

/however

however for some time.

((2)) PROGRESS REPORT ON NAVAL CODE FOR 1/11/44

The examination of the book groups recovered in October has not yet led to any decisive success in judging their correctness.

V ~~TOP SECRET~~

OKM

4/SKL III Fm 2/11/44

To: 4/SKL III

((1)) PROGRESS REPORT FOR "DELIVERY GROUPS"

SITUATION AS ON 1/11/44

Apart from current work, in which nothing fundamentally fresh was observed, an investigation is being made whether the evaluation of delivery groups dealt with so far by the main Naval D/F Station KARERSEE (previously MONTPELLIER), can be used as a firm basis for identifying convoys from and to the MEDITERRANEAN. Results have so far been negative. Investigations are, however, being continued as to whether the delivery groups can supply data for the recognition of convoys. A final report cannot be made until later.

((2)) PROGRESS REPORT FOR TURKEY

SYSTEM, SITUATION AS ON 1/11/44.

Study discontinued, as monitoring of the Turkish frequencies produced no results.

Trans. K.C.K.
J.M.E.